McAfee Agent 4.5
Product Guide

Contents

Contents

About the McAfee Agent

The term *agent* is used in three different contexts:

- McAfee Agent
- SuperAgent
- Agent Handler

McAfee Agent

The McAfee Agent is the client-side component that provides secure communication between McAfee managed products and ePolicy Orchestrator. The agent also provides local services to these products and to products developed by McAfee's Security Innovation Alliance partners. While enabling products to focus on enforcing their policies, the McAfee Agent delivers services that include updating, logging, reporting events and properties, task scheduling, communication and policy storage.

The agent is installed on the systems you intend to manage with ePolicy Orchestrator. Systems can only be managed by ePolicy Orchestrator with an agent installed.

While running silently in the background, the agent:

- Gathers information and events from managed systems and sends them to the ePO server.
- Installs products and upgrades on managed systems.
- Enforces policies and schedules tasks on managed systems and sends events back to the ePO server.
- Updates security content such as the DAT files associated with McAfee VirusScan.

SuperAgent

A SuperAgent is an agent that can broadcast wake-up calls to other ePO agents located on the same network broadcast segment (usually identical with a network subnet). Each SuperAgent then pings the agents in its subnet. Agents located in a segment with no SuperAgent do not receive the wake-up call. This is an alternative to sending ordinary agent wake-up calls to each agent in the network, and the advantage is that it can distribute network traffic.

SuperAgents can also serve as the repository of distributable software and updates for those agents in its broadcast segment. Additionally, the agent's global updating feature relies entirely upon SuperAgent wake-up calls to perform its function.

Agent Handler

An Agent Handler is the ePO component responsible for managing communication between agent and server. Beginning with ePolicy Orchestrator 4.5, Agent Handlers can be installed on other computers to provide fault tolerant and load-balanced communication to many agents, including geographically distributed agents.

Agent-server communication

During agent-server communication, the agent and server exchange information using a propietary network protocol (for ePO 4.0) or an industry-standard network protocol TLS (for ePO 4.5) that ePolicy Orchestrator uses for secure network transmissions. At each communication, the agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the agent, and the repository list if it has changed since the last agent-server communication. The agent enforces the new policies locally on the managed system and applies any task or repository changes.

Agent-server communication can be initiated in these ways:

* Agent-to-server communication interval (ASCI) lapses.

* Agent-initiated communication upon agent startup.

* Agent wake-up calls from ePO or Agent Handlers.

* Communication initiated manually from the managed system (Windows only).

Agent-server communication interval

The agent-server communication interval (ASCI) is set on the General tab of the McAfee Agent policy page. This setting determines how often the agent calls in to the server. The default setting of 60 minutes means that the agent contacts the server once every hour.

When deciding whether to modify the interval, consider the following:

* At each ASCI, the following actions occur:

  * The agent collects and sends its properties to the server or Agent Handler.

  * The agent sends the events that have occurred since the last agent-server communication.

  * The server or Agent Handler sends new policies and tasks to the client. This action might dictate other resource-consuming actions, such as an immediate DAT download.

  * The agent enforces policies.

* Although these activities do not burden any one computer, the cumulative demand on the network, on ePO servers, or on Agent Handlers can be significant, considering these variables:

  * The number of systems being managed by ePolicy Orchestrator.

  * Your organization's threat response requirements.

  * The network or physical location of clients in relation to servers or Agent Handlers.

  * Available bandwidth.

In general, the more these variables reflect conditions that are likely to burden or slow down your network, the less frequently you want to perform an agent-server communication. For clients with critical functions, you might want to set a more frequent interval.

If you decide to change these settings, the McAfee Agent policy page is found by clicking **Menu | Policy | Policy Catalog**, selecting **McAfee Agent**, then clicking **Edit Settings**.

Agent-initiated communication after agent installation

After the agent is installed, it calls in to the server at a randomized interval within ten minutes. Thereafter, the agent calls in at each agent-server communication interval (ASCI). By default, agent-server communication occurs every 60 minutes.

You can force the agent to communicate with the server at any time after installation by clicking the McAfee system tray icon, (if it has been enabled), and selecting **McAfee Agent Status Monitor**. When the Monitor appears, clicking **Collect and Send Props** sends full or minimal properties as defined on the General page of the McAfee Agent Policy Catalog. Clicking **Send Events** transmits events to the server but does not transmit policies and tasks from the server.

NOTE: For information on enabling the system tray icon see *Using the system tray icon*.

If the system tray icon has not been enabled, you can access the status monitor at the command prompt. Set the working directory to the McAfee Common Framework folder (the default location is C:\Program Files\McAfee\Common Framework), then type this command:

CmdAgent.exe /s

Wake-up calls and wake-up tasks

Communication between the ePO server and the agent takes place at regular intervals set by the ePO administrator. The purpose of an agent wake-up call is to trigger an immediate agent-server communication rather than wait for the next agent-server communication, which is set at 60 minutes by default. There are two ways to issue a wake-up call:

- Directly from the server — This is the most common approach and requires the presence of an open port on the client.
- On a schedule set by the administrator — This approach is useful when agent-server communication has been disabled on the General tab of the McAfee Agent policy catalog. The administrator can create and deploy a wake-up *task*, which triggers a wake-up *call* on a schedule.

Some reasons for issuing an agent wake-up call are:

- There has been a change in policy that you want the agent to adopt immediately, without waiting for the next ASCI.
- You have created a new task that you want the agent to run immediately.
- A query has generated a report indicating that a client is out of compliance, and you want to test its status as part of a troubleshooting procedure.

If you are running Microsoft Windows and have converted a particular system to use as a SuperAgent, it can issue wake-up calls to designated network broadcast segments. SuperAgents distribute the bandwidth impact of the agent wake-up call, and help distribute network traffic.

If you decide to change these settings, the McAfee Agent policy page is found by clicking **Menu | Policy | Policy Catalog**, selecting **McAfee Agent**, then clicking **Edit Settings**.

SuperAgents and broadcast wake-up calls

If you operate in a Windows environment and plan to use agent wake-up calls to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent.

SuperAgents distribute the bandwidth load of concurrent wake-up calls. Instead of sending agent wake-up calls from the server to every agent, the server sends the SuperAgent wake-up call to SuperAgents in the selected System Tree segment. When SuperAgents receive this wake-up call, they send broadcast wake-up calls to all agents in their network broadcast segments.

The process is:

1 Server sends a wake-up call to all SuperAgents.

2 SuperAgents broadcast a wake-up call to all agents in the same broadcast segment.

3 All agents (regular agents and SuperAgents) exchange data with the server.

4 An agent without an operating SuperAgent on its broadcast segment is not prompted to communicate with the server.

To deploy enough SuperAgents to the appropriate locations, first determine the broadcast segments in your environment and select a system (preferably a server) in each segment to host a SuperAgent. Be aware that agents in broadcast segments without SuperAgents do not receive the broadcast wake-up call, so they do not call in to the server in response to a wake-up call.

Agent and SuperAgent wake-up calls use the same secure channels. Ensure that:

• The agent wake-up communication port (8081 by default) is not blocked.

• The agent broadcast communication port (8082 by default) is not blocked.

NOTE: Client firewalls might block communication from the ePO server. Ensure that the ports required for communication from the ePO server are not block by a firewall on the client.

System requirements and supported operating systems and processors

This section specifies the system requirements for McAfee Agent 4.5 and the operating systems and processors it supports.

System requirements

• Installed disk space — 29-32 MB, excluding log files

• Memory — 256 MB RAM

• Processor speed — 500 MHz minimum

Supported operating systems and processors

Operating systems	Processor
Apple Macintosh OS X Tiger	• Intel • PowerPC
Apple Macintosh OS X Leopard	• Intel • PowerPC
HP-UX 11i v1 (build 11.11)	PA-RISC
HP-UX 11i v2 (build 11.23)	
IBM AIX 5.3 (TL8 or later)	Power 5
IBM AIX 6.1	Power 5
McAfee Email and Web Security 3100	Not applicable
McAfee Email and Web Security 3200	
Red Hat Linux Enterprise 4	x86, x64 or compatible
Red Hat Linux Enterprise 5	

Operating systems	Processor
Solaris 8; 32-bit or 64-bit	SPARC
Solaris 9; 32- bit or 64-bit	
Solaris 10; 64-bit	
SuSE Linux 8.2	x86, x64 or compatible
SuSE Enterprise Server 9	
SuSE Enterprise Server 10	
Windows 2003 Server R2; 32-bit; Enterprise, Standard, or Web Editions; SP 1 or 2	• Itanium 2 • Intel Pentium • Intel Celeron (recommended) or compatible • x86, x64 or compatible
Windows 2003 Server R2; 64-bit; Enterprise, Standard, or Web Editions; SP 2	
Windows Vista Home Premium; 32-bit or 64-bit; GA, SP 1 or 2	• Intel Pentium • Intel Celeron (recommended) or compatible • x86, x64 or compatible
Windows Vista Home Basic; 32-bit or 64-bit; GA, SP 1 or 2	
Windows Vista Business; 32-bit or 64-bit; GA, SP 1 or 2	
Windows Vista Enterprise; 32-bit or 64-bit; GA, SP 1 or 2	
Windows Vista Ultimate; 32-bit or 64-bit; GA, SP 1 or 2	
Windows 2008 Server Standard; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server Enterprise; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server Datacenter; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server Web; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server Core; 32-bit or 64-bit; GA or SP 2	
Windows XP Home Edition; 32-bit or 64-bit; SP2 or 3	
Windows XP Professional; 32-bit or 64-bit; SP2 or 3	
Windows XP Tablet PC Edition; 32-bit or 64-bit; SP3	

NOTE: The agent is compatible with Windows operating systems that provide Data Execution Prevention (DEP).

Installing the McAfee Agent

The installation procedure for the McAfee Agent varies depending on:

- The operating system in use — Windows, Solaris, HB-UX, Macintosh, or Linux.
- The type of installation — First-time installation or upgrade on a system already hosting an agent.
- The tools used to install — ePolicy Orchestrator native tools, login scripts, images, or none.

This section provides instructions on installing the agent in a variety of environments.

Methods of agent deployment and installation

The terms *deployment* and *installation* both describe the process of equipping one or more computers with the McAfee Agent. However, there is a difference:

- *Installation* means placing the agent on a computer where no agent is present. Administrator privileges are required to install the agent.
- *Deployment* means placing the agent, or managed products and their upgrades, on one or more computers where an agent is already present.

If you are operating in a Windows environment, you can push install or update the agent directly from the ePO console. Alternatively, you can copy the agent installation package onto removable media or into a network share for manual or login script installation on your Windows systems.

However, you cannot push the installation package to UNIX-based systems. Here, the agent must be installed manually using an installation script (install.sh) that ePO creates when you check in the agent to the ePO master repository and indicate the operating system in use. Once the agent is in place on the client computers, you can run an agent deployment task to schedule updates to the agent as well as deploy products for management by ePO.

NOTE: The procedure described for agent installation on UNIX-based systems can be used in Windows environments as well, if preferred

This table lists methods for installing and deploying the agent. The first three methods are installing the agent and might require the use of embedded credentials. The remaining five methods are deploying the agent and do not require embedded credentials.

Method	Action	Notes
Installing the agent		
Manually	The network administrator installs the agent on each managed system individually.	- Aside from using third-party deployment products, this is the only method available for the initial installation on UNIX systems. - Once the agent is installed, you can use ePolicy Orchestrator to

Method	Action	Notes
		upgrade products and update product content..
Using third-party software such as Microsoft Systems Management Server (SMS) or IBM Tivoli	Configure your third-party software to distribute the agent installation package, which is located on your ePO server.	• The agent installation package contains necessary security keys and the site list. • See third-party instructions.
Using login scripts (Windows only)	The network administrator creates an installation or upgrade script, which runs at each logon to a system.	• The user must log on to the system to trigger the installation or upgrade. • The installation package must be in a location accessible to the system.
Deploying the agent: A deployment task is created in ePolicy Orchestrator and is sent to the client where it runs. If the repository contains a newer version of the agent, the deployment task pull down the newer version and installs it over the existing version.		
Using ePolicy Orchestrator	The ePO administrator specifies the systems and selects **Push Agents...** when adding a new system.	• Selecting a large number of systems can temporarily affect network throughput. • You must specify credentials with administrator rights to the target systems.
Upgrading agents using the deployment task	Use the ePO System Tree to upgrade the agent on selected target systems.	• Requires that an agent is already present on the target system.
Deploying an image containing the agent (Windows)	Administrator creates an image that contains the agent and deploys the image. Before creating the image, the administrator removes the agent GUID and MAC address from the agent section of the registry.	• Removing the GUID and MAC address allows the agent to generate a new GUID and MAC address upon the first agent-server communication. • Failure to remove the GUID and MAC address results in "sequencing errors" from the multiple identical systems
Enabling the agent on unmanaged McAfee products (Windows)	Using the System Tree, the ePO administrator selects the systems to be converted from unmanaged status to managed status and selects **Actions □ Agent □ Deploy Agents**.	• Requires an agent on the target system in unmanaged mode.
Enabling the agent on unmanaged McAfee products (UNIX-based platforms)	Type the following command on the system containing the agent you want to enable: /opt/McAfee/cma/bin/msaconfig -m -d <Path of location containing **srpubkey.bin** , **reqseckey.bin** and **SiteList.xml**> [-nostart]	• You must have root privileges to perform this action. • You must use the **srpubkey.bin**, **reqseckey.bin** and **SiteList.xml** files from the ePO server.

Installing on Windows from ePolicy Orchestrator

You must have administrator privileges on the Windows system to perform this task. The agent extension must be installed on the ePolicy Orchestrator server before the agent is installed on any clients.

1   Download both the agent extension, **ePOAgentMeta.zip** and the agent package, **MA450Win.zip** to the system containing the ePO server.

2   Install the agent extension:

   a   Click **Menu | Software | Extensions**. The Extensions page opens.

   b   Click **Install Extension**.

   c   Browse to the location containing **ePOAgentMeta.zip**, select it and click **OK**. The Install Extensions summary page appears.

   d   Click **OK** to complete the installation of the extension.

3   Check in the agent package to the ePolicy Orchestrator repository.

   NOTE: If installing on a computer running Common Management Agent 3.6, the package must be checked in to the **Current** repository branch.

   a   In ePolicy Orchestrator, click **Software**.

   b   Click **Check In Package**.

   c   Browse to **MA450Win.zip**, select it and click **Next**.

   d   If **Allow package check-in for any repository branch** has been enabled, place the package any branch. To enable this feature, click **Menu | Configuration | Server Settings**, then select **Repository Packages** from the list of Setting Categories. Click **Edit** to toggle from No to Yes.

   e   Click **Save**.

4   Push the agent to client systems by following these steps:

   a   Click **Menu | Systems | System Tree**.

   b   Select the target systems or groups.

   c   Click **Actions**, select **Agent** from the pop-up menu, then select **Deploy Agents** from the submenu. The Deploy McAfee Agent page appears.

   d   Select the version of the agent to be deployed.

   e   If needed, select installation options:

      •   **Install only on systems that do not already have an agent managed by this ePO server**

      •   **Force installation over existing version**(Not recommended)

   f   Define the installation path for the agent: select a prefix from the drop-down menu, then accept the folder name that appears or type a new one.

   g   Type valid credentials in the **Domain**, **User name**, and **Password** fields.

   h   Click **OK**.

Installing on Windows using third-party deployment methods

The agent extension must be installed on the ePO server before the agent is installed on any target systems. McAfee recommends that you refer to the release notes to verify that you are using the most current package and extension.

TIP: This task requires the creation of an agent installation package, FramePkg.exe (see Step 4). Installation of the package requires administrator credentials.

Task

For option definitions, click **?** in the interface.

1   Download both the agent extension, **ePOAgentMeta.zip**, and the agent package, **MA450Win.zip**, to the system containing the ePO server.

2   Install the agent extension:

    a   Click **Menu | Software | Extensions**. The Extensions page opens.

    b   Click **Install Extensions**.

    c   Browse to the location containing **ePOAgentMeta.zip**, select it and click **OK**. The Install Extensions summary page appears.

    d   Click **OK** to complete the installation of the extension.

3   Check in the agent package to one of the repository branches, **Current** (default), **Previous**, or **Evaluation**.

    a   In ePolicy Orchestrator, click **Software**.

    b   Click **Check In Package**.

    c   Browse to **MA450Win.zip**, select it and click **Next**.

    d   If **Allow package check-in for any repository branch** has been enabled, place the package any branch. To enable this feature, click **Menu | Configuration | Server Settings**, then select **Repository Packages** from the list of Setting Categories. Click **Edit** to toggle from No to Yes.

    e   Click **Save**.

4   Create an installation package:

    a   Click **Menu | Systems | System Tree**. The System Tree page opens.

    b   Click **System Tree Actions**, then select **New Systems** from the drop-down menu.

    c   Select **Create and download agent installation package**.

    d   Deselect **Use Credentials**.

    NOTE: If deselected, you receive the default package. If selected you can specify required credentials.

    e   Click **OK**. The Download file dialog box opens.

    f   Select **FramePkg.exe** and save it to the desktop.

5   To embed credentials, modify the local security policy on the target systems:

    a   Log on to the target system using an account with local administrator permissions.

    b   From the command line, run SECPOL.MSC to open the Local Security Settings dialog box.

    c   In the System Tree under **Security Settings | Local Policies**, select **User Rights Assignment**.

    d   In the Policy column of the details pane, double-click **Impersonate a client after authentication** to open the Local Security Policy Setting dialog box.

    e   Click **Add User or Group...** to open the Select Users or Groups dialog box.

    f   Select the user or group that the user is likely to run as (for example, **Everyone** or **Users**), then click **OK**.

    g   Click **OK**. You are now ready to use your third-party software to distribute **FramePkg.exe**.

Installing the agent manually

Use these instructions to install agents manually.

Tasks

▶ Installing on Windows manually

▶ Installing on UNIX-based operating systems

Installing on Windows manually

This method is appropriate if your organization requires that software is installed on systems manually. You can install the agent on the system, or distribute the FramePkg.exe installer for users to run the installation program themselves. If you want users (who have local administrator rights) to install the agent on their own systems, distribute the agent installation package file to them. You can attach it to an email message, copy it to media, or save it to a shared network folder.

After the agent is installed, it calls in to the server and adds the new system to the System Tree.

Task

For option definitions, click **?** in the interface.

1 Distribute the agent installation package to the target system.

2 Double-click **FramePkg.exe**.

   NOTE: You may be prompted with a Security Warning by Windows. Click **Run** to continue. Wait a few moments while the agent is installed.

3 Click **OK** to complete the installation.
   Within ten minutes, the agent calls in to the ePO server for the first time.

4 As needed, bypass the ten-minute interval by forcing the agent to call. Use this command:

   CMDAGENT /p

   NOTE: Systems on which McAfee Agent is installed manually will initially be located in the **Lost & Found** group of the ePO System Tree.

Installing on UNIX-based operating systems

Use this task to install the agent on AIX, HP-UX, Linux, Macintosh, and Solaris systems. The agent extension must be installed on the ePO server before the agent is installed on any target systems.

Before you begin

• You must have root privileges on the UNIX-based system to complete this task

Task

1 Download ePOAgentMeta.zip to a temporary location on the ePO server.

2 Open the ePOAgentMeta.zip and extract the agent package for the target operating system.

Operating system	File name
HP-UX	MA450HPX.zip
Linux	MA450LNX.zip
Macintosh	MA450MAC.zip
Solaris	MA450SLR.zip
AIX	MA450AIX.zip

3 Install the agent extension on the ePO server.

   a Click **Menu | Software | Extensions**, then click **Install extension**.

   b Browse to the location containing **ePOAgentMeta.zip**, select it and click **OK**. The Install Extensions summary page appears.

   c Click **OK** to complete the installation of the extension.

4 Check in the agent package to one of the repository branches, **Current** (default), **Previous**, or **Evaluation**.

   a In ePolicy Orchestrator, click **Software**.

   b Click **Check In Package**.

   c Browse to **MA450Win.zip**, select it and click **Next**.

   d If **Allow package check-in for any repository branch** has been enabled, place the package any branch. To enable this feature, click **Menu | Configuration | Server Settings**, then select **Repository Packages** from the list of Setting Categories. Click **Edit** to toggle from No to Yes.

   e Click **Save**.

5 From the selected repository branch, copy the **install.sh** file to the target systems.

   TIP: The path includes the name of the selected repository. For example, if checked in to the Current branch of the ePO software repository, the path of the required files is:

Operating System	Location
AIX	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT4000AIXX\Install\0409
HPUX	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT4000HPUX\Install\0409
Linux	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700LYNX\Install\0409
Macintosh	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700MACX\Install\0409
Solaris	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700SLRS\Install\0409

6 Log on to the target system as "root."

7 Open **Terminal**, then switch to the location where you copied the install.sh file.

8 Run these commands:

   chmod +x install.sh

   ./install.sh -i

Creating custom agent installation packages

Use this task to create a custom agent installation package.

If you use a distribution method other than ePolicy Orchestrator deployment capabilities (such as login scripts or third-party deployment software), you can create a custom agent installation package (FramePkg.exe or install.sh) with embedded administrator credentials. This is necessary in a Windows environment if users do not have local administrator permissions. The user account credentials you embed are used to install the agent.

NOTE: Microsoft Windows XP Service Pack 2 and later do not allow embedded administrator credentials until the package file name has been added to the exception list of the Windows firewall.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Systems | System Tree**. The System Tree page opens.

2   Click **System Tree Actions**, then select **New Systems** from the drop-down menu.

3   Next to **How to add systems**, select **Create and download agent installation package**.

4   Deselect **Use Credentials**.

5   Select the appropriate operating system.

6   Type the appropriate **Credentials for agent installation**, then click **OK**.

7   When prompted, select the file to be downloaded. Click to open the file. Right-click to save the file.

8   Distribute the custom installation package file as needed.

Installing the agent with login scripts

Use this Windows only task to set up and use network login scripts to install the agent on Windows systems as they log on to the network.

Using network login scripts is a reliable method to make sure that every system logging on to your network is running an agent. You can create a login script to call a batch file that checks if the agent is installed on systems attempting to log on to the network. If no agent is present, the batch file installs the agent before allowing the system to log on. Within 10 minutes of being installed, the agent calls in to the server for updated policies and ePO tasks, and the system is added to the System Tree.

This method is appropriate when:

• Domain names or sorting filters are assigned to the segments of your System Tree.

• You already have a managed environment and want to ensure that new systems logging on to the network become managed as a result.

• You already have a managed environment and want to ensure that systems are running a current version of the agent.

Before you begin

• McAfee recommends first creating segments of your System Tree that use either network domain names or sorting filters that add the expected systems to the desired groups. If you don't, all systems are added to the Lost&Found group, and you must move them manually.

- Consult your operating system documentation for writing login scripts. The details of the login script depend on your needs. This task uses a basic example.
- Create a batch file (ePO.bat) that contains commands you want to execute on systems when they log on to the network. The content of the batch file depends on your needs, but its purpose is to check whether the agent has been installed in the expected location and, if not, run FramePkg.exe to install the agent. Below is a sample batch file that does this.

  IF EXIST "C:\Program Files\McAfee\Common Framework\FRAMEWORKSERVICE.EXE" GOTO END_BATCH

  \\MyServer\Agent\UPDATE$\FRAMEPKG.EXE /INSTALL=AGENT

  :END_BATCH

  NOTE: The installation folders for your distribution might be different than in this example, depending on where you have specified to install the agent.

  This example checks:

  - The default installation folder for an agent file and, if not present, installs the new agent.

Task

For option definitions, click **?** in the interface.

1 Copy the agent installation package, FramePkg.exe, from your ePO server to a shared folder on a network server, where all systems have permissions.

  Systems logging on to the network are automatically directed to this folder, to run the agent installation package and install the agent. The default location for the agent installation packages for Windows is: C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe

2 Save the batch file you created, ePO.bat, to the NETLOGON$ folder of your primary domain controller (PDC) server. The batch file runs from the PDC every time a system logs on to the network.

3 Add a line to your login script that calls the batch file on your PDC server. The line would look similar to this example:

  CALL \\PDC\NETLOGON$\EPO.BAT

  Each system runs the script when it logs on to the network and, if necessary, installs the agent.

Including the agent on an image

When you include the McAfee Agent on an image, you must remove its GUID from the registry. This allows subsequently installed agent images to generate their own GUID at their first agent-server communication.

CAUTION: If you don't follow this step, all deployed agent images have the same GUID, and must be changed manually. In a large organization, this is impractical. Although you can configure the ePO server to identify replicated GUIDs and assign a new GUID at the next agent-server communication, the action consumes considerable processing bandwidth. For information, see *Identifying and correcting a duplicate GUID*.

Task

On the imaged system, locate the registry key for the agent and remove it. The registry keys are located at:

HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent\AgentGUID

Identifying and correcting a duplicate GUID

If you deployed the agent on an image without first removing its GUID from the registry, multiple systems in your environment will have duplicate GUIDs. When these systems fail to communicate with the Agent Handler, they generate sequencing errors, which indicate a GUID problem. The Managed Systems query result type tracks the following information about these errors:

- The number of sequence errors for each system in the Managed Systems Sequence Errors property.
- The date and time of the last sequence error in the Managed Systems Last Sequence Error property.

The tracked information is incorporated into one or the other of the available pre-defined queries:

- Systems with High Sequence Errors
- Systems with no Recent Sequence Errors

Two predefined tasks help manage GUID problems.

- **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**

  This task deletes the systems that have a large number of sequencing errors and classifies the agent GUID as problematic. As a result, the agent is forced to generate a new GUID. The threshold number of sequencing errors is set in the query Systems with High Sequence Errors.

- **Duplicate Agent GUID - Clear error count**

  Sequencing errors can occur occasionally for inconsequential reasons. This task clears the count of sequencing errors in systems that have not had any recent sequencing errors. This cleanup task does not remove any problematic GUIDs. The threshold value for defining *recent* is set in the query Systems with no Recent Sequence Errors

Use this task to identify computers with GUID problems and take corrective action.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Automation | Server Tasks** to open the Server Tasks Builder.

2 Click **Edit** for one or the other of the following tasks.

- **Duplicate Agent GUID - Clear error count**
- **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**

3 In the Description page, select **Enabled**, then click either **Save** or **Next.**

- If you click **Save**, the task runs with the default configuration displayed on the **Actions** and **Schedule** tabs. If you want to configure a schedule for this task, click **Next**. This allows you to review the Action settings and then set a schedule.
- If you click **Next**, the Actions page appears. This page has been preconfigured to correspond to the requirements of the Duplicate Agent GUID task that you selected in Step 2. Ensure that the following settings are displayed:

	Duplicate Agent GUID - Clear error count	Duplicate Agent GUID - remove systems with potentially duplicated GUIDs
Actions	Run Query	Run Query
Query	Systems with no Recent Sequence Errors	Systems with High Sequence Errors

	Duplicate Agent GUID - Clear error count	Duplicate Agent GUID - remove systems with potentially duplicated GUIDs
Sub-Actions	Clear Agent GUID Sequence Error Count	Move Agent GUID to Duplicate List and Delete Systems

- Click **Next** again to display the Schedule page. Specify the frequency, start and end dates, and time for running this query.

4   Click **Save**.

TIP: You can run either of the tasks immediately by selecting **Run** in the Actions column on the Server Tasks page.

Scheduling corrective action for a duplicate GUID

If you have deployed the agent on an image without first having removed its GUID from the registry, multiple systems in your environment will have duplicate GUIDs. When these systems fail to communicate with the Agent Handler, they generate sequencing errors, indicating a GUID problem.

Use this task to automatically identify duplicate agent GUIDs, and schedule their removal.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Automation | Server Tasks**, then click **Edit** in the row labeled **Duplicate Agent GUID - remove systems**. The Server Task Builder wizard opens.

2   On the Description page, select **Enabled**.

- To run the task with the default configuration displayed on the Actions and Schedule tabs, click **Save**.

- To configure the Actions and Schedule tabs, click **Next**. The Actions page appears.

3   From the Actions drop-down menu, select **Run Query**.

4   Next to the Query field, click the **...** button, select one of the following options, then click **OK**.

- **System with high Sequence errors**

- **Systems with no recent Sequence errors**

5   From the Sub-Actions drop-down menu, select one of these options, then click **Next**.

- **Clear Agent GUID Sequence Error Count**

- **Move Agent GUID to Duplicate List and Delete systems**

6   Set a schedule for running the task, then click **Next**.

7   Review your settings, then click **Save**.

Deploying the agent via push technology

Use this task to deploy agents to your Windows systems using ePolicy Orchestrator.

This method is recommended if large segments of your System Tree are already populated. For example, if you created System Tree segments by importing domains or Active Directory containers, and you chose not to deploy the agent during the import.

Before you begin

To use this method, these requirements must be met:

• Systems must already be added to the System Tree.

  NOTE: If you have not yet created the System Tree, you can deploy the agent installation package to systems at the same time that you add groups and systems to the System Tree. However, McAfee does not recommend this procedure if you are importing large domains or Active Directory containers. Those activities generate significant network traffic.

• The account specified must have local administrator privileges on all target systems. Domain administrator rights are required on a system to access the default Admin$ shared folder. The ePO server service requires access to this shared folder in order to install agents.

• The ePO server must be able to communicate with the desired systems.

  Before beginning a large agent deployment, ping some targets by machine name to verify that the server can communicate with a few systems in each segment of your network. If the targeted systems respond to the ping, ePolicy Orchestrator can reach the segments.

  NOTE: The ability to successfully use ping commands from the ePO server to managed systems is not required for the agent to communicate with the server. It is, however, a useful test to determine if you can deploy agents from the server.

• The Admin$ share folder on target systems must be accessible from the ePO server. Verify that this is true on a sample of target systems. This test also validates your administrator credentials, because you cannot access remote Admin$ shares without administrator rights.

  From the ePO server, click **Start | Run**, then type the path to the target system's Admin$ share, specifying either system name or IP address. For example, type \\<System Name>Admin$.

  If the systems are properly connected over the network, and your credentials have sufficient rights, and the Admin$ share folder is present, a Windows Explorer dialog box appears.

• Network access must be enabled on Windows XP Home systems. Deploy the agent from ePolicy Orchestrator or install a custom agent installation package on systems running Windows XP Home.

Task

For option definitions, click **?** in the interface.

1 Download the agent extension, **ePOAgentMeta.zip**, and the agent package, **MA450Win.zip**, to the system containing the ePO server.

2 Install the agent extension:

  a Click **Menu | Software | Extensions**. The Extensions page opens.

  b Click **Install Extensions**.

  c Browse to the location containing **ePOAgentMeta.zip**, select it, then click **OK**. The Install Extensions summary page appears.

  d Click **OK** to complete the installation of the extension.

3 Check in the agent package to the ePolicy Orchestrator repository.

  NOTE: If installing on a computer running Common Management Agent 3.6, the package must be checked in to the Current repository branch.

  a Click **Menu | Software | Master Repository**. A list of packages in the repository appears.

      b Click **Actions**, then select **Check In Package** from the drop-down menu.

      c Browse to **MA450Win.zip**, select it, then click **Next**.

      d Ensure that **Current** is selected in the Branch field, then click **Save**.

4 Push the agent to target systems:

      a Click **Menu | Systems | System Tree**, then select the groups or systems where you want to deploy the agent.

      b Click **Actions**.

      c Select **Agent** from the first pop-up menu, then select **Deploy Agents** from the second drop-down menu.

      d From the **Agent version** drop-down list, select an agent version.

      e Select one of these options:

        • **Install only on systems that do not already have an agent managed by this ePO server**

        • **Force installation over existing version**

      NOTE: If you use the force installation option, the agent is removed in its entirety, including policies, tasks, events, and logs before the new agent is installed.

      f Type valid credentials in the **Domain**, **User name**, and **Password** fields.

      g Click **OK**.

Enabling and disabling the agent on unmanaged McAfee products

Before acquiring ePolicy Orchestrator, you might have already been using McAfee products in your network. Some of the more recent McAfee products that use AutoUpdate, such as VirusScan Enterprise, are installed with the agent in *updater* mode. To start managing these products with ePolicy Orchestrator, you can enable the agent that is already on the system.

Enabling the agent on each system saves significant network bandwidth over deploying the agent installation package. However, existing McAfee products were probably installed with an older version of the agent, and these agents are *not* automatically upgraded to the latest version on the ePO server.

In some situations, you may want to convert a system that has been managed by ePolicy Orchestrator to updater (unmanaged) mode. Information is provided for converting from managed mode to unmanaged mode.

Use these tasks to enable agents on existing McAfee products in your environment so that they work with ePolicy Orchestrator or to disable management of systems by ePolicy Orchestrator.

Tasks

▶ Converting the agent mode from unmanaged to managed mode in Windows

▶ Converting the agent mode from unmanaged to managed on UNIX-based platforms

▶ Converting the agent mode from managed to unmanaged mode in Windows

▶ Converting the agent mode from managed to unmanaged on UNIX-based platforms

Converting the agent mode from unmanaged to managed mode in Windows

Use this task to convert the agent from unmanaged (updater) mode to managed mode in a Windows environment.

Before you begin

Before converting the agent mode, consider the following:

- By default, the FrmInst.exe file is installed in this location: C:\Program Files\McAfee\Common Framework.

- You should not change the agent installation folder without removing and reinstalling the agent. Agents that you enable might be in a different folder than agents that you deploy in your network by another method.

- Assigning sorting filters or domain names to specific System Tree segments saves time. Without such designations, systems are placed in **Lost&Found** and you will have to move them from that location.

- You must copy the SiteList.xml (repository list file) from the ePO server to the target systems. The repository list contains network address and other information that the agent requires to call in to the server after being installed.

- SiteList.xml must be in the same location as srpubkey.bin and reqseseckey.bin.

Two methods for performing this task are provided.

Method A

This method, although simple and fast, involves sending a 5 MB file across the network.

1 Export Framepkg.exe to a temporary location on the target system, (that is, the system to be converted from unmanaged to managed mode.) See *The agent installation package* for information on creating this file.

2 Run Framepkg.exe.

Method B

This method is complex and time consuming but involves using only 400 KB of network bandwidth.

1 Copy sitelist.xml, srpubkey.bin and reqseckey.bin from the ePO server to a temporary location on the target system.

2 Run C:\Program Files\McAfee\Common Framework\frminst.exe on the target system.

Converting the agent mode from unmanaged to managed on UNIX-based platforms

Use this task to convert the agent from unmanaged (updater) mode to managed mode on a UNIX-based platform.

NOTE: This procedure can be used to change which ePO server or Agent Handler an agent communicates with.

Task

1 On the target system, locate the **msaconfig** file in the binaries subfolder of the **cma** folder. For example, on HP-UX, Linux, and Solaris systems, the location is /opt/McAfee/cma/bin. On Macintosh systems, the location is /Library/McAfee/cma/bin.

2 Run /opt/McAfee/cma/bin/msaconfig -m -d <path of location containing srpubkey.bin, reqseckey.bin and SiteList.xml> [-nostart].

   NOTE: Optional -nostart indicates that the agent does not restart after changing mode.

Converting the agent mode from managed to unmanaged mode in Windows

Use this task to convert the agent from managed mode to unmanaged (updater) mode in a Windows environment.

Task

1 Click **Menu □ Systems □ System Tree**.

2 Select the systems to convert.

3 Click **Actions □ Directory Management □ Delete.**

4 Confirm the deletion. The selected system is no longer managed by ePolicy Orchestrator and now functions only as an updater.

Converting the agent mode from managed to unmanaged on UNIX-based platforms

Use this task to convert the agent from managed mode to unmanaged (updater) mode on a UNIX-based platform.

Task

1 On the target system, locate the **msaconfig** file in the binaries subfolder of the **cma** folder. For example, on HP-UX, Linux, and Solaris systems, the default location is /opt/McAfee/cma/bin. On Macintosh systems, the default location is /Library/McAfee/cma/bin.

2 Run /opt/McAfee/cma/bin/msaconfig -u [-nostart].

   NOTE: Optional [-nostart] indicates that the agent does not restart after changing mode.

Agent installation folder — Windows

The default location of the agent installation folder is the same on managed systems and on the ePO server.

• <System_Drive>\Program Files\McAfee\Common Framework

Agent installation folder — UNIX-based systems

Installation of the agent on UNIX-based operating systems generates files in these locations:

Operating system	Location	Contents
AIX	/opt/McAfee/cma/	All binaries, logs, agent working area
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/usr/sbin/	cma Script for starting and stopping the agent, manually and when called by the system.
HP-UX	/opt/McAfee/cma/	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/sbin/init.d/cma	cma Script for starting and stopping the agent, manually and when called by the system.
Linux	/opt/McAfee/cma/	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/etc/init.d/	cma Script for starting and stopping the agent, manually and when called by the system.
Macintosh	/Library/McAfee/cma	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/Library/StartupItems/cma/	cma Script for starting and stopping the agent, manually and when called by the system.
Solaris	/opt/McAfee/cma/	All binaries, logs, agent working area.

Operating system	Location	Contents
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/etc/init.d/	cma Script for starting and stopping the agent, manually and when called by the system.

The agent installation package

A FramePkg.exe file is created when you install ePolicy Orchestrator and whenever you check in an agent package. It is a customized installation package for agents that report to your server. The package contains information necessary for the agent to communicate with the server. Specifically, this package includes:

- The agent installer
- SiteList.xml file
- srpubkey.bin (the server public key)
- reqseckey.bin (the initial request key)

By default, the path of the agent installation package on the server is:

C:\Program Files\McAfee\ePolicy
Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe

This is the installation package that the server uses to distribute and install agents. Other FramePkg.exe files are created when:

- Agent packages are checked in to any branch of the repository (Previous, Current, or Evaluation)
- Encryption key changes

The default agent installation package contains no embedded user credentials. When executed on the targeted system, the installation uses the account of the currently logged-on user.

Agent installation command-line options

Depending on whether the agent is already installed, you can use command-line options when you run the agent installation package (FramePkg.exe) or the agent framework installation (FrmInst.exe) program.

You can employ these command-line options when using the deployment task to upgrade to a new version of the agent.

This table describes all of the agent installation command-line options. These options are *not* case-sensitive, but their values are.

FramePkg.exe and FrmInst.exe command-line options

Command	Description
/DATADIR	Specifies the folder on the system to store agent data files. The default location is: <Documents and Settings>\All Users\Application Data\McAfee\Common Framework. If the operating system does not have a Documents and Settings folder, the default location is C:\ProgramData\McAfee\Common Framework Sample: FRAMEPKG /INSTALL=AGENT /DATADIR=<AGENT DATA PATH>
/DOMAIN/ USERNAME/ PASSWORD	Specifies a domain, and account credentials used to install the agent. The account must have rights to create and start services on the desired system. If left unspecified, the credentials of the currently logged-on account are used. If you want to use an account that is local to the desired system, use the system's name as the domain. Sample: FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=jdoe /PASSWORD=password
/FORCEINSTALL	Specifies that the existing agent is uninstalled, then the new agent is installed. Use this option only to change the installation directory or to downgrade the agent. When using this option, McAfee recommends specifying a different directory for the new installation (/INSTDIR). Sample: FRAMEPKG /INSTALL=AGENT /FORCEINSTALL /INSTDIR=c:\newagentdirectory
/INSTALL=AGENT	Installs and enables the agent. Sample: FRAMEPKG /INSTALL=AGENT
/INSTALL=UPDATER	Enables the AutoUpdate 7.0 component if it has already been installed, and does not change whether the agent is enabled. This command-line option upgrades the agent. Sample: FRAMEPKG /INSTALL=UPDATER
/INSTDIR	Specifies the installation folder on the desired system. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default location is: <DRIVE>:\program files\mcafee\common framework Sample: FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent
/REMOVE=AGENT	Removes the agent if not in use. If in use, the agent changes to *updater* mode. Sample: FRMINST /REMOVE=AGENT
/SILENT or /S	Installs the agent in silent mode, hiding the installation from the end user. Sample: FRAMEPKG /INSTALL=AGENT /SILENT
/SITEINFO	Specifies the folder path to a specific repository list (SiteList.xml) file. Sample: FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\TMP\SITELIST.XML
/USELANGUAGE	Specifies the language version of the agent that you want to install. If you select 0409 or a locale other than the 12 languages with locale IDs, the software appears in English. If you install multiple language versions, the locale selected in operating system determines the language version that displays. Sample: FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404

Assigning values to custom properties

Use this task to specify up to four custom properties during installation of the agent at the command line. These values override values set by the ePO administrator.

Custom properties are reported back to the ePO server and are displayed in the system properties. These properties can be used to enhance custom reporting on systems or to allow custom tagging.

Task

- At the command line, type the string that is appropriate for your operating system:

  - **Windows operating systems:** FrmInst.exe /CustomProp1="Property 1" /CustomProp2="Property 2" /CustomProp3="Property 3" /CustomProp4="Property 4"

    NOTE: In Windows, custom property values are stored in the registry at

    HKLM\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent\CustomProps\

  - **UNIX-based operating systems:** msaconfig -CustomProp1 "Property 1" -CustomProp2 "Property 2" -CustomProp3 "Property 3" -CustomProp4 "Property 4"

    NOTE: Custom property values are stored in CustomProps.xml, an editable file located at /McAfee/cma/scratch/.

Upgrading and Restoring Agents

Use these tasks to upgrade or restore existing agents in your environment.

If you have been using an older version of ePolicy Orchestrator and have previous agent versions in your environment, you can upgrade those agents once you've installed your new ePO server. The procedure for upgrading the agent depends on which agent version is running on your managed systems.

NOTE: Some previous agent versions do not support all functions in ePolicy Orchestrator 4.5. For full ePolicy Orchestrator functionality, upgrade to agent version 4.5 or later.

Tasks

▶ Upgrading agents using product deployment task

▶ Upgrading agents manually or with login scripts

▶ Restoring a previous version of the agent (Windows)

▶ Restoring a previous version of the agent (UNIX)

Upgrading agents using product deployment task

Use this task to deploy a newer version of the agent with the Product Deployment client task. This is the same task that is used to deploy products, such as VirusScan Enterprise, to systems that are already running agents.

Periodically, McAfee releases newer versions of the agent, which can be deployed and managed using ePolicy Orchestrator. When the agent installation package is available, you can download it from the McAfee download site, check it in to the master repository, then use the deployment task to upgrade the agent.

NOTE: The term *upgrading* is not the same as *updating*. *Upgrading* the agent means installing a newer version of the agent over an older version, for example, replacing McAfee Agent 4.0 with McAfee Agent 4.5. *Updating* means getting the most up-to-date DATs and signatures that products use to identify and disarm threats.

Before you begin

- If you use ePolicy Orchestrator to deploy agents in your network, the procedure differs slightly depending which previous version of the agent you are upgrading.

- If you are upgrading your agents and your network is very large, consider the size of the agent installation package file and your available bandwidth before deciding how many agents to upgrade at once. Consider using a phased approach. For example, upgrade one group in your System Tree at a time. In addition to balancing network traffic, this approach makes tracking progress and troubleshooting any issues easier.

- If you use a product deployment client task to upgrade agents, consider scheduling the task to run at different times for different groups in the System Tree.

Task

For option definitions, click **?** in the interface.

1 Ensure that the desired agent installation package is checked in to the desired branch of the master repository.

2 Click **Menu | Systems | System Tree**.

3 Click the **Client Tasks** tab.

4 Click **Actions**, then select **New Task** from the drop-down menu. The Client Task Builder wizard opens to the Description page.

5 Name the task, then select **Product Deployment** from the drop-down list and select whether the task should be sent to all computers or to tagged computers.

6 Click **Next**. The Configuration page appears.

7 Select the target platform.

8 Use the drop-down lists in the Products and Components area to specify the version of the agent to deploy and, if needed, additional command-line parameters.

9 If you are working in a Windows environment, select whether to run the task at each policy enforcement interval.

10 Click **Next** to open the Schedule page.

11 Schedule the task as needed, then click **Next**. The Summary page appears.

12 Verify the task's details, then click **Save**. The new deployment task is sent to the client computers at the next agent-server communication. Thereafter, every time the task executes, it checks to determine whether it should install the specified agent.

Upgrading agents manually or with login scripts

If you don't use ePolicy Orchestrator to deploy agents to managed systems, you can use your preferred agent distribution method to upgrade existing agents. Upgrading agents by a method other than using ePolicy Orchestrator, such as upgrading manually or using network login scripts, is the same as installing agents for the first time. You must distribute the FramePkg.exe installation file and launch it on the system using your preferred method. For more information, see Methods of agent deployment and installation.

Restoring a previous version of the agent (Windows)

Use this task to restore a previous version of the agent in a Windows environment. You might do this to test a new version of the agent.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Systems | System Tree**, then select the systems you want to downgrade.

2 Click **Actions**, select **Agent**, then select **Deploy Agents**. The Deploy Agent page appears.

3 From the **Agent version** drop-down list, select the agent you want to restore.

4 Select **Force installation over existing version.**

5 Specify the target installation path for the forced installation.

6 Enter user credentials for agent installation.

7 Provide the **Number of attempts**, **Retry interval**, and **Abort after** information.

8 Select whether the connection used for the deployment is to use a selected Agent Handler or all Agent Handlers.

9 Click **OK** to send the agent installation package to the selected systems.

Restoring a previous version of the agent (UNIX)

Use this task to restore a previous version of the agent in a UNIX environment. You might do this to test a new version of the agent.

Task

For option definitions, click **?** in the interface.

1 Uninstall the currently installed version of the agent. For details, see *Uninstalling from UNIX-based operating systems*.

2 Install the earlier version of the agent. For details, see *Installing the agent manually*.

NOTE: Tasks, policies and other data are restored at the first agent-server communication following reinstallation.

Configuring Agent Policies

Agent policy general settings are specified on the Policy Catalog pages of the ePolicy Orchestrator console, including policies for events, logging, repositories, updates, and proxy.

▶ About agent policy settings

▶ Proxy settings for the agent

▶ Retrieving system properties

▶ Scheduling a client task for a group

▶ Creating a new scheduled client task

▶ Configuring selected systems for updating

About agent policy settings

Agent policy settings determine the performance and behavior of an agent in your environment. The interface provides 6 configuration pages for setting policy options:

- **General**, where the following policies are set:
  - Policy enforcement interval
  - Use of system tray icon
  - Agent and SuperAgentwake-up call support in Windows environments
  - The repository path where the agent goes for product and update packages
  - Whether to accept connections only from the ePO server
  - Creation of SuperAgents
  - Rebooting options
  - Agent-server communication
  - Sending full or minimal system properties and product properties
- **Events**, where priority event forwarding is set. (See *Priority event forwarding*).
- Logging, where the following policies are set:
  - Enabling/disabling of logging
  - Level of logging detail
  - Setting remote access to logging
- **Repositories**, where repository selection variables are set. (See *Selecting a repository*).
- **Updates**, where the following policies are set:
  - Identifying log file information
  - Specifying post-updating executables
  - Downgrading DAT files

- Defining repository branches
- **Proxy**, where proxy settings are specified. (See *Proxy settings for the agent*).

Before distributing a large number of agents throughout your network, consider carefully how you want the agent to behave in the segments of your environment. Although you can configure agent policy settings after agents are distributed, McAfee recommends setting them prior to the distribution, to prevent unnecessary impact on your resources.

For complete descriptions of all options on the agent policy pages, click **?** on the page displaying the options.

Priority event forwarding

During normal operation, the agent and security software on the managed system generate software events regularly. These events can range from information about regular operation, such as when the agent enforces policies locally, to critical events, such as when a virus is detected and not cleaned. These events are uploaded to the server at each agent-server communication and are stored in the database. A typical deployment of agents in a large network can generate thousands of these events an hour.

You can configure the agent to forward events on a priority basis if they are equal to or greater than a specified severity. Specific event severities are determined by the product generating the events. If you plan to use Automatic Responses, McAfee recommends that you enable priority uploading of higher severity events for those features to function as intended.

You can enable priority uploading of events on the Events tab of the McAfee Agent policy pages.

Selecting a repository

Use this task to set the policy for repository selection. The agent can update from any repository in its repository list based on the policy setting. This repository management tool allows you to specify the most efficient means for designating a source repository for updates.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Policy Catalog**.

2   Select **McAfee Agent** from the Product drop-down menu and ensure that **General** is selected in the Category drop-down menu.

3   Click **Actions**, then select **New Policy** to create a new policy or **My Default** policy to edit your policy.

4   Type a name for the policy, then click **OK**.

5   On the Repositories tab, select whether to **Use this repository list** (the ePO-managed repository list, SiteList.xml), or **Use other repository list** (a locally controlled repository list that is not managed by ePolicy Orchestrator).

6   Choose a basis for selecting a repository:

Selection Method	Definition
Ping time	The shortest round-trip elapsed time between sending an echo request to a remote ICMP-enabled system and receiving a response from that system. Ping timeout can be used to control the maximum time taken. Minimum = 5 seconds; maximum = 60 seconds. The default is 30 seconds.

Selection Method	Definition
Subnet distance	The fewest hops an ICMP packet makes while traversing the network from a local system to a remote system. The maximum number of hops can be used to control the packet traversal. The default is 15.
Use order in repository list	A user-defined list of repositories based on locally determined preferences. You can sequence and enable or disable specific distributed repositories on the Repositories tab of the McAfee Agent policy pages. Allowing agents to update from any distributed repository ensures that they get the update from some location.

NOTE: The agent selects a repository each time a change occurs in the repository list, IP address, or policy option.

Proxy settings for the agent

To access the McAfee update sites, the agent must be able to access the Internet. Use the agent policy settings to configure proxy server settings for managed systems. The Proxy tab of the McAfee Agent policy pages includes these settings:

- **Do not use a proxy** (default setting)
- **Use Internet Explorer proxy settings** — This setting allows an agent in a Windows environment to use the proxy server and credential information currently configured for Internet Explorer. There are several methods to configure Internet Explorer for use with proxies. For information, see Internet Explorer Help.

  NOTE: When this setting is selected, the fields for specifying user authentication for HTTP and FTP proxies become available, as well as the option **Allow user to configure proxy settings**. By selecting this option, the administrator grants permission to the user of a managed product to access additional update repositories that are configured behind the proxy server.

- **Configure the proxy settings manually** — When this setting is selected, the fields for specifying user authentication for HTTP and FTP proxies and exceptions become available. This selection also allows the administrator to specify the HTTP and FTP locations using **DNS name**, **IPv4** address, or **IPv6** address.

Configuring proxy settings for the agent

Use this task to specify whether to use proxies.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Policy | Policy Catalog**, then from the Product drop-down menu, select **McAfee Agent**, and from the Category drop-down menu, select **General**.

2   From the list of policies select the **Edit Settings** link on the row labeled My Default, .

3   Click **Proxy**. The proxy settings page appears.

4   Select your preferred option:

- If your agent does not require a proxy to access the Internet, select **Do not use a proxy**. This is the default selection.

- On Windows systems you can select **Use Internet Explorer proxy settings** and if appropriate, select **Allow user to configure proxy settings**.
- If you need a proxy other than Internet Explorer, select **Configure the proxy settings manually**.

5 Select a form for the address of the source HTTP or FTP location where the agent is to pull updates. The DNS Name drop-down menu includes the address options **DNS Name** (the fully-qualified domain name), **IPv4** and **IPv6** notation.

6 Type the DNS name or IP address and Port numbers of the HTTP and/or FTP source. If appropriate, select **Use these settings for all proxy types**.

7 Select **Specify exceptions** to designate systems that do not require access to the proxy.

8 Select **Use HTTP proxy authentication** and/or **Use FTP proxy authentication**, then provide a user name and credentials.

9 Click **Save**.

Retrieving system properties

Use this task to retrieve system properties from managed systems.

At each agent-server communication, the agent sends information to the ePO server about the managed computer, including information about the software products that are installed. The scope of the information depends on how you have configured:

- The agent policy that specifies whether to retrieve a full set of information about installed programs, or only a minimal set.
- The task setting that specifies whether to retrieve all properties defined by the agent policy, or only properties that have changed since the last agent-server communication. This setting is available when configuring an immediate or scheduled wake-up call.

For detailed information on how to access the configuration settings for retrieving properties of the managed system and of the products installed, see *Accessing settings to retrieve properties*. For a list of properties, see *Windows system and product properties reported by the agent*. To create a wake-up task, see *Creating a new scheduled client task*.

Task

NOTE: Use the agent **General** policy page to set minimal or full product properties. Select or deselect **Send full product properties in addition to system properties**. If deselected, only minimal product properties are sent in addition to system properties.

To retrieve system properties *plus…*	Do this. . .
Minimal product properties that have changed since the last agent-server communication	**1** Set the agent policy to send minimal product properties.
	2 Set the wake-up task to send only properties that have changed since the last communication.
Full product properties that have changed since the last agent-server communication	**1** Set the agent policy to send full product properties.
	2 Set the wake-up task to send only properties that have changed since the last communication.

Minimal product properties whether or not they have changed since the last agent-server communication	**1**	Set the agent policy to send minimal product properties.
	2	Set the wake-up task to send all properties, as defined by the agent policy.
Full product properties whether or not they have changed.	**1**	Set the agent policy to send full properties.
	2	Set the wake-up task to send all properties, as defined by the agent policy.

Scheduling a client task for a group

Use this task to schedule a client task for a group.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Systems | System Tree | Client Tasks**.

2 In the System Tree, select the group to be configured.

3 In the Actions field, click **Edit Settings** for the task to be configured. The Client Task Builder wizard opens.

4 Select **Break inheritance and assign the policy and setting below this point**.

5 On the **Schedule** page:

   a Enable the task.

   b Set the schedule, frequency, and options for the task.

   c Click **Next** to review your settings.

6 Click **Save**. At the next agent-server communication, the task is sent to the group's members.

Creating a new scheduled client task

Use this task to create a new client task that runs on a schedule, such as a mirror task, update task, and McAfee Agent wake-up task.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Systems | System Tree**.

2 Select **Client Tasks**, then click **Actions** and select **New Task** from the drop-down menu. The Client Task Builder wizard opens.

3 On the **Description** page:

   a Type a name for the task and any notes that might be useful.

   b From the drop-down menu, select the kind of task you are creating.

   c Indicate whether to send the task to all systems or to only systems that have certain tags or have no tags.

      d Click **Next**.

4 On the **Configuration** page:

- For a mirror task, type the location on the managed systems where you want to replicate contents from the repository. The repository is selected based on policy selections on the Repositories tab of the agent policy pages.

- For an update task, indicate if the update progress dialog box is visible on managed systems and if users can postpone the update. You can also indicate if all packages in the repository are included or only selected packages.

- For an agent wake-up task, indicate whether to send only properties that have changed since the last agent-server communication, or all properties defined by the agent policy.

5 Click **Next**.

6 On the **Schedule** page:

      a Enable the task.

      b Set the schedule, frequency, and options for the task.

      c Click **Next** to review your settings.

7 Click **Save**.

Configuring selected systems for updating

Use this task to specify which update packages are updated immediately when Update Now is selected. Typical reasons for using this functionality include:

- Updating selected systems when troubleshooting

- Distributing new DATs or signatures to a large number of systems, or all systems, immediately

- Updating selected products that have been deployed previously

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Systems | System Tree | Systems**, then select the systems to be updated.

2 Click **Actions**, select **Agent**, then select **Update Now**.

- Select **All packages** to deploy all update packages in the repository.

- Select **Selected packages** to specify which update packages to deploy. Deselect the packages that you do not want to deploy.

3 Click **OK.**

Working with the agent from the ePO server

The ePO interface includes pages where agent tasks and policies can be configured, and where agent properties can be viewed.

Use these tasks when working with the agent from the ePO server.

Tasks

▶ Viewing agent and product properties

▶ Viewing system information

▶ Accessing settings to retrieve properties

▶ Windows system and product properties reported by the agent

▶ Sending manual wake-up calls to systems

▶ Sending manual wake-up calls to a group

▶ Making the system tray icon visible

▶ Locating inactive agents

Viewing agent and product properties

Use this task to verify that the properties match the policy changes you have made. This is useful for troubleshooting. The available properties depend on whether you configured the agent to send full or minimal properties on the McAfee Agent policy pages.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Systems | System Tree**.

2   Select a system. Information about the system's properties, installed products, and agent appear.

Viewing system information

Use this task to view information about a selected system, including a list of its managed products.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Systems | System Tree**.

2   Click the system whose information you want to view. The System Details page appears.

3 Scroll through the list of available information, including a field labeled **Installed Products**.

4 Click the **More** link to see detailed properties for each installed product.

Accessing settings to retrieve properties

Use these tasks to access the settings used for retrieving properties.

Task

For option definitions, click **?** in the interface.

To do this...	Do this...
Set agent policy	**1** Click **Menu | Systems | System Tree | Assigned Policies | <Product = McAfee Agent> | Edit Assignment | Edit Policy**. **2** Select or deselect **Send full product properties in addition to system properties**. If deselected, only minimal product properties are sent in addition to system properties.
Send an immediate agent wake-up call	**1** Click **Menu | Systems | System Tree | <select target systems> | Actions | Agent | Wake Up Agents**. **2** Select **Get full product properties in addition to system properties** if you need them.
Set the scheduled wake-up call	**1** Click **Menu | Systems | System Tree | Client Tasks | <select a wake-up task or create a New Task> | Type = McAfee Agent Wakeup | Next**. **2** Select **Send all properties defined by the agent policy** or **Send only properties that have changed since the last agent-server communication**. **3** Set the Schedule.

Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

Agent Version	IPX Address	Subnet Address
CPU Serial Number	Is 64 Bit OS	Subnet Mask
CPU Speed (MHz)	Last Communication	System Description
CPU Type	MAC Address	System Location
Custom Props 1-4	Managed State	System Name
Default Language	Number Of CPUs	System Tree Sorting
Description	Operating System	Tags
DNS Name	OS Build Number	Time Zone
Domain Name	OS OEM Identifier	Total Disk Space
Free Disk Space	OS Platform	Total Physical Memory
Free Memory	OS Service Pack Version	User Name
Installed Products	OS Type	
IP Address	OS Version	

Product properties

Each McAfee product designates the properties it reports to ePolicy Orchestrator and, of those, which are included in a set of minimal properties. This list shows the kinds of product data that are reported to ePolicy Orchestrator by the McAfee software installed on your system. If you find errors in the reported values, review the details of your products before concluding that they are incorrectly reported.

Agent Wake-Up Communication Port

Agent-to-Server Communication Interval

DAT Version

Engine Version

HotFix/Patch Version

Language

License Status

Policy Enforcement Interval

Product Version

Service Pack

Sending manual wake-up calls to systems

Use this task to manually send an agent or SuperAgent wake-up call to systems in the System Tree. This is useful when you make policy changes and you want agents to call in for an update before the next agent-server communication.

Before you begin

Before sending the agent wake-up call to systems, make sure that **Enable agent wake-up call support** is enabled and applied on the General tab of the McAfee Agent policy pages. It is enabled by default.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Systems | System Tree**, then select the group that contains the target systems.

2   Select the systems from the list, click **Actions**, select **Agent**, then select **Wake Up Agents** from the submenu. The Wake Up McAfee Agent page appears.

3   Ensure that the systems you selected appear in the Target section.

4   Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call**.

5   Accept the default **Randomization** (0 - 60 minutes) or type a different value. Consider the number of systems that are receiving the wake-up call, and how much bandwidth is available. If you type 0, agents respond immediately.

6   During regular communication, the agent sends only properties that have changed since the last agent-server communication. This task is set by default to **Get full product properties...**. To send the complete properties as a result of this wake-up call, ensure that this is option selected.

7   Click **OK** to send the agent or SuperAgent wake-up call.

Sending manual wake-up calls to a group

Use this task to manually send an agent or SuperAgent wake-up call to a System Tree group. This is useful when you have made policy changes and want agents to call in for an update.

Before you begin

Make sure that wake-up support for the targeted group is enabled and applied on the General tab of the McAfee Agent policy pages. It is enabled by default.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Systems | System Tree**.

2   Click **Group Details**, then select the target group from the System Tree.

3   Click **Actions**, then select **Wake Up Agents**. The Wake Up McAfee Agent page appears.

4   Verify that the group appears next to **Target group**.

5   Select whether to send the agent wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.

6   Next to **Type**, select whether to send an **Agent wake-up call** or **SuperAgent wake-up call**.

7   Accept the default **Randomization** (0 - 60 minutes), or type a different value. If you type 0, agents awaken immediately.

8 During regular communication, the agent sends only properties that the point-products designate as important. This task is set by default to **Get full product properties...**. To send the complete properties as a result of this wake-up call, ensure that this is option selected.

9 Click **OK** to send the agent or SuperAgent wake-up call.

Making the system tray icon visible

Use this task to make the McAfee system tray icon visible on managed computers.

Task

1 Click **Menu | Systems | System Tree | Assigned Policies | <Product = McAfee Agent>**.

2 Click a policy, for example **McAfee Default**. The McAfee Agent General tab for the selected policy opens.

3 Select **Show the McAfee system tray icon (Windows only)**.
You can also select **Allow end users to update security from the McAfee system tray menu**. When selected, users who are running McAfee Agent 4.5 can choose **Update Security** from the McAfee system tray icon to update all products for which an update package is present in the repository.

4 When you have completed your changes to the default configuration, click **Save**.

Locating inactive agents

An inactive agent is one that has not communicated with the ePO server within a user-specified time period. Some agents might become disabled or be uninstalled by users. In other cases, the system hosting the agent might have been removed from the network. McAfee recommends performing regular weekly searches for systems with these inactive agents.

To perform the search, run the ePolicy Orchestrator query named **Managed Inactive Agents**. (For information on queries, see *Queries* in the ePolicy Orchestrator Product Guide.) The default configuration of this query reports systems that have not communicated with the ePO server in the last month. You can specify hours, days, weeks, quarters or years.

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication. The query results allow you take a variety of actions with respect to the systems identified, including ping, delete, wake up, re-deploy an agent, etc.

CAUTION: If you force install a new agent, all previous policies and settings are lost.

Running agent tasks from the managed system

Use these tasks to perform selected procedures from the system where the agent is installed.

If you can access the managed system where the agent is installed, you can view and manage some features of the agent.

NOTE: The agent interface is available on the managed system only if you selected **Show McAfee system tray icon** and **Allow end users to update security from the McAfee System tray menu** on the General tab of the McAfee Agent policy pages.

Tasks
- ▶ Running a manual update
- ▶ Enforcing policies
- ▶ Updating policies
- ▶ Sending properties to the ePO server
- ▶ Sending events to the ePO server immediately
- ▶ Using the icon option to update
- ▶ Forcing the agent to call in to the server
- ▶ Viewing version numbers and settings
- ▶ Agent command-line options

Running a manual update

Use this Windows-only task to run an update manually from the managed system.

Task

1 On the managed system, right-click the McAfee system tray icon.

2 Select **Update Security**. The agent performs an update from the repository defined in the agent policy.

Product updates can include:

- • Patch releases
- • Legacy product plug-in (.DLL) files
- • Service pack releases
- • SuperDAT (SDAT*.EXE) packages
- • Supplemental detection definition (ExtraDAT) files
- • Detection definition (DAT) files
- • Anti-virus engines

- Managed-product signatures

Enforcing policies

Use this Windows-only task to prompt an agent to enforce all configured policies on the managed system.

Task

1   On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.

2   Click **Enforce Policies**. The policy enforcement activity is displayed in the Agent Status Monitor.

Updating policies

Use this Windows-only task to prompt the agent on the managed system to call in to the server to update policy settings.

Task

1   On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.

2   Click **Check New Policies**. The policy-checking activity is displayed in the Agent Status Monitor.

Sending properties to the ePO server

Use this Windows-only task to send properties to the ePO server from the managed system.

Task

1   On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.

2   Click **Collect and Send Props**. A record of the property collection activity is added to the list of activities in the Agent Status Monitor.

NOTE: The agent policy controls whether full or incremental properties are sent.

Sending events to the ePO server immediately

Use this Windows-only task to send events to the server immediately from the managed system.

Task

1   On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.

2 Click **Send Events**. A record of the sending-events activity is added to the list of activities in the Agent Status Monitor.

NOTE: This action sends all events to ePolicy Orchestrator irrespective of their severity.

Using the icon option to update

For the administrator to control what is updated and when, the Windows-only option for users to **Update Security** is disabled by default. If you want to allow Windows users to update all McAfee products on their managed systems, you must enable this functionality. See *Configuring selected systems for updating* for more information. The icon cannot be used to update applications selectively. The user can update all the items in the repository, or none of them.

When the user selects **Update Security**, all of the following items are updated with the contents of the designated repository:

- Patch releases
- Legacy product plug-in (.DLL) files
- Service pack releases
- SuperDAT (SDAT*.EXE) packages
- Supplemental detection definition (ExtraDAT) files
- Detection definition (DAT) files
- Anti-virus engines
- Managed-product signatures

Forcing the agent to call in to the server

Use this Windows-only task to force the new agent to call in to the ePO server immediately. You can do this from any system on which an agent has just been installed. This is useful after installing the agent manually.

Task

1 On the system where you installed the agent, open a DOS command window by selecting **Start** | **Run**, type cmd, and press **Enter**.

2 In the command window, navigate to the agent installation folder containing the CmdAgent.exe file.
By default, this is C:\Program Files\McAfee\Common Framework.

3 Type this command:
CMDAGENT /p

4 Press **Enter**. The agent calls into the server immediately.

When the agent calls in to the server for the first time, the system is added to the System Tree as a managed system. If you configured criteria-based sorting for the System Tree, the system is added to the location appropriate for its IP address or tags. Otherwise, the system is added to the Lost&Found group. Once the system is added to the System Tree, you can manage its policies through ePolicy Orchestrator.

Viewing version numbers and settings

Use this task to view the agent settings from the managed system and to look up the version numbers of the agent and product from the managed system. This is useful for troubleshooting when installing new agent versions, or to confirm that the installed agent is the same version as the one displayed in the agent properties on the server.

Task

1 On the managed system, right-click the McAfee system tray icon.

2 Select **About** to view information about the agent:

- Computer name
- Agent version number
- ePO Server DNS Name
- ePO Server IP Address
- ePO Server Port Number
- Agent ID (GUID)
- Date and time of last security update
- Time lapse since last agent-to-server communication
- Agent-to-server communication interval
- Policy enforcement interval
- Management state (managed, unmanaged, or SuperAgent)

In addition, information identifies the McAfee products installed and under management by ePolicy Orchestrator.

Agent command-line options

Use the Windows-only Command Agent (CmdAgent.exe) tool to perform selected agent tasks from the managed system. CmdAgent.exe is installed on the managed system at the time of agent installation. Perform this task locally on managed systems using this program or the McAfee system tray icon.

The CmdAgent.exe file is located in the agent installation folder. By default, this location is:

C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

Command-line parameters

Parameter	Description
/C	Checks for new policies. The agent contacts the ePO server for new or updated policies, then enforces them immediately upon receipt.
/E	Prompts the agent to enforce policies locally.
/P	Sends properties and events to the ePO server.
/S	Displays the Agent Monitor and its options.

Using the system tray icon

In a Windows environment, if the agent policy has been set to show the McAfee icon in the system tray of the managed system, the user can access shortcuts to information and functionality of managed products.

▸ What the system tray icon does

▸ Making the system tray icon visible

▸ Enabling user access to updating functionality

What the system tray icon does

Option	Function
About...	Displays system and product information for products installed on the system, including the agent, the ePO server with which the agent communicates, and the software products being managed.
Quick Settings	Links to product menu items that are frequently used.
Manage Features	Displays links to the administrative console of managed products.
Update Security	Triggers immediate updating of all installed McAfee software products. This includes application of patches and hotfixes, as well as DAT and signature updates. NOTE: This feature is available only if specifically enabled in the agent policy.
Scan Computer for	Launches McAfee programs, such as VirusScan, that scan systems on-demand and detect unwanted malicious software.
View Security Status	Displays the current system status of managed McAfee products, including current events.
McAfee Agent Status Monitor	Triggers the Agent Status Monitor, which: • Displays information on the collection and transmission of properties. • Sends events. • Downloads and enforces policies.

Making the system tray icon visible

Use this task to make the McAfee system tray icon visible on managed computers.

Task

1   Click **Menu | Systems | System Tree | Assigned Policies | <Product = McAfee Agent>**.

2   Click a policy, for example **McAfee Default**. The McAfee Agent General tab for the selected policy opens.

3   Select **Show the McAfee system tray icon (Windows only)**.
You can also select **Allow end users to update security from the McAfee system tray menu**. When selected, users who are running McAfee Agent 4.5 can choose **Update Security** from the McAfee system tray icon to update all products for which an update package is present in the repository.

4   When you have completed your changes to the default configuration, click **Save**.

Enabling user access to updating functionality

Use this task to allow users to update through the system tray icon.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Policy | Policy Catalog | <Product = McAfee Agent>**.

2   Click **Edit Settings** in the row containing the policy to be modified. The McAfee Agent General tab for the selected policy opens.

3   Select **Allow end users to run update security from the McAfee system tray menu**.

4   When you have completed your changes to the default configuration, click **Save**.

Removing the McAfee Agent

Use these tasks to remove agents from systems.

After deleting an agent, it is deleted from the System Tree and the agent removed during the next agent-server communication. Keep in mind that if point products still reside on systems after attempting to remove the agent, the agent will continue to run unmanaged in updater mode in order to maintain those point products.

NOTE: You cannot remove the agent using the Product Deployment task, which can remove products such as VirusScan Enterprise.

Tasks

▸ Running FrmInst.exe from the command line

▸ Removing agents when deleting systems from the System Tree

▸ Removing agents when deleting groups from the System Tree

▸ Removing agents from systems in query results

▸ Uninstalling from non-Windows operating systems

Running FrmInst.exe from the command line

Use this task to remove the agent from a system by running the agent installation program, FrmInst.exe, from the command line.

NOTE: If there are point-products installed on a system from which the agent has been removed, the now unmanaged agent continues in updater mode.

Task

- Run the agent installation program, FrmInst.exe, from the command line with the /REMOVE=AGENT option. The default location of this file is:
  C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

Removing agents when deleting systems from the System Tree

Use this task to remove agents from systems when you delete those systems from the System Tree.

Task

For option definitions, click **?** in the interface.

1. Click **Menu | Systems | System Tree**, then select the group with the systems you want to delete.

2. Select the systems from the list, then click **Actions**.

3. Select **Directory Management** from the drop-down menu, then select **Delete** from the submenu.

4. Confirm the deletion, then click **OK**.

Removing agents when deleting groups from the System Tree

Use this task to remove agents from all systems in a group when you delete that group from the System Tree.

CAUTION: When you delete a group, all of its child groups and systems are also deleted.

Task

For option definitions, click **?** in the interface.

1. Click **Menu | Systems | System Tree**, then select a group to be deleted.

2. At the bottom of the System Tree panel, click **System Tree Actions** then select **Delete Group**.

3. Select **Remove agent from all systems**, then click **OK**.

Removing agents from systems in query results

Use this Windows-only task to remove agents from systems listed in the results of a query (for example, the Agent Versions Summary query).

Task

For option definitions, click **?** in the interface.

1. Run the desired query, then, from the results page, select the systems to be deleted.

2. Select **Directory Management** from the drop-down menu, then select **Delete** from the submenu.

3. Confirm the deletion, then click **OK**.

Uninstalling from non-Windows operating systems

Use this task to remove the agent from HP-UX, Linux, Macintosh, and Solaris systems. The task involves:

• Removing the agent from the system.

• Removing the system name from the ePO System Tree.

Task

1 Log on as "root" to the system where you want to remove the agent.

2 Run the command appropriate for your operating system.

Operating System	Commands
AIX	rpm -e MFEcma
HP-UX	swremove MFEcma
Linux	rpm -e MFEcma rpm -e MFErt NOTE: Be certain to follow the order listed here.
Macintosh	/Library/McAfee/cma/uninstall.sh
Solaris	pkgrm MFEcma

3 Click **Menu | Systems | System Tree**, then select the systems you have uninstalled.

4 From the Actions drop-down menu, select **Directory Management**, then select **Delete** from the submenu.

Agent Activity Logs

The agent log files are useful for determining agent status or for troubleshooting. Two log files record agent activity and are located in the agent installation folders on the managed system.

Agent activity log

This log file records agent activity related to things such as policy enforcement, agent-server communication, and event forwarding. You can define a size limit of this log file. On the Logging tab of the McAfee Agent policy pages, you can configure the level of agent activity that is recorded.

The agent activity log is an XML file named agent_<system>.xml, where <system> is the NetBIOS name of the system where the agent is installed.

Detailed agent activity log

In addition to the information stored in the agent activity log, the detailed activity log contains troubleshooting messages. This file has a 1 MB default size limit. When this log file reaches 1 MB, a backup copy is made (agent_<system>_backup.log).

On Windows systems, the detailed agent activity log is named agent_<system>.log file, where <system> is the NetBIOS name of the system on which the agent is installed.

On UNIX-based systems, the detailed log files are found in the folder /opt/McAfee/cma/scratch/etc and they are named log, log.1, log.2,…, log.5. The higher the log number, the older the file.

Viewing the agent activity log

Use these tasks to view the agent activity log. This log file records an agent's activity. The amount of detail depends on the policy settings you select on the Logging tab of the McAfee Agent policy pages.

These log files can be viewed from the managed system or from the ePO interface.

Tasks
▸ Viewing the agent activity log from the managed system
▸ Viewing the agent activity log from the ePO server

Viewing the agent activity log from the managed system

Use this task to view the agent activity log from the system where the agent is installed.

Task

NOTE: The agent icon is available in the system tray only if the **Show McAfee system tray icon (Windows only)** option is selected on the General tab of the McAfee Agent policy pages. If it is not visible, select this option and apply it. When you finish viewing the log file content, you can hide the icon again by deselecting the option and applying the change.

1   On the managed system, right-click the McAfee Agent icon in the system tray, then select **Status Monitor**. The Status Monitor displays the agent activity log.

2   When finished viewing the agent activity log, close the Status Monitor.

Viewing the agent activity log from the ePO server

Use this task to view the agent activity log of a system from the ePO server.

Before you begin

Be sure that the McAfee Agent policy settings are set to the following:

• Accept connection only from ePO server is unchecked (McAfee Agent policy pages, General tab)

• Enable remote access to log is checked (McAfee Agent policy pages, Logging tab)

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Systems | System Tree**, then select the system.

2   From the Actions drop-menu, select **Agent**, then select **Show Agent Log**.

3   To view the backup copy of the detailed log, click **previous**.

Index